# Varnost omrežij

## 1 Orodja za spremljanje prometa v omrežju

Zagotavljanje varnosti komunikacij in omrežij si težko zamišljamo brez zmogljivih orodij za spremljanje stanja in prometa (dogajanja) v omrežju in vanj priključenih napravah.

### Orodja ukazne vrstice Windows

Namenjena so predvsem za preverjanje in spreminja omrežnih nastavitev računalnika. Med najbolj uporabnimi so:

- ipconfig
- netstat
- net

### Naloge:

Odprite ukazno vrstico računalnika in izvedite spodnje naloge:

1. Z ukazom **ipconfig -?** preverite vse možnosti tega orodja.
   a. Poiščite ukaz s katerim izpišete vse podrobnosti mrežnih vmesnikov vašega računalnika.
   b. Poiščite in uporabite ukaz s katerim ponastavite mrežne nastavitve računalnika.
2. Z ukazom **netstat -?** preverite vse možnosti tega orodja.
   a. Poiščite ukaz s katerim izpišete statistiko na vmesniku Ethernet.
   b. Izpišite samo aktivne TCP povezave.
   c. Izpišite usmerjevalno tabelo računalnika.
   d. Izpišite kateri programi sodelujejo v vzpostavljenih povezavah.
3. Z ukazom **net help** preverite vse možnosti tega orodja.
   a. Z ukazom **net use** preverite uporabo mrežnih virov.
   b. Z ukazom **net view** preverite kateri računalniki so priključeni v omrežje.

### Analizator prometa in protokolov Wireshark

Z a analizo prometa na računalniku priključenem v omrežje, uporabimo program Wireshark. Če ga na računalniku še ni, ga prenesemo s strani http://www.wireshark.org/ in namestimo.

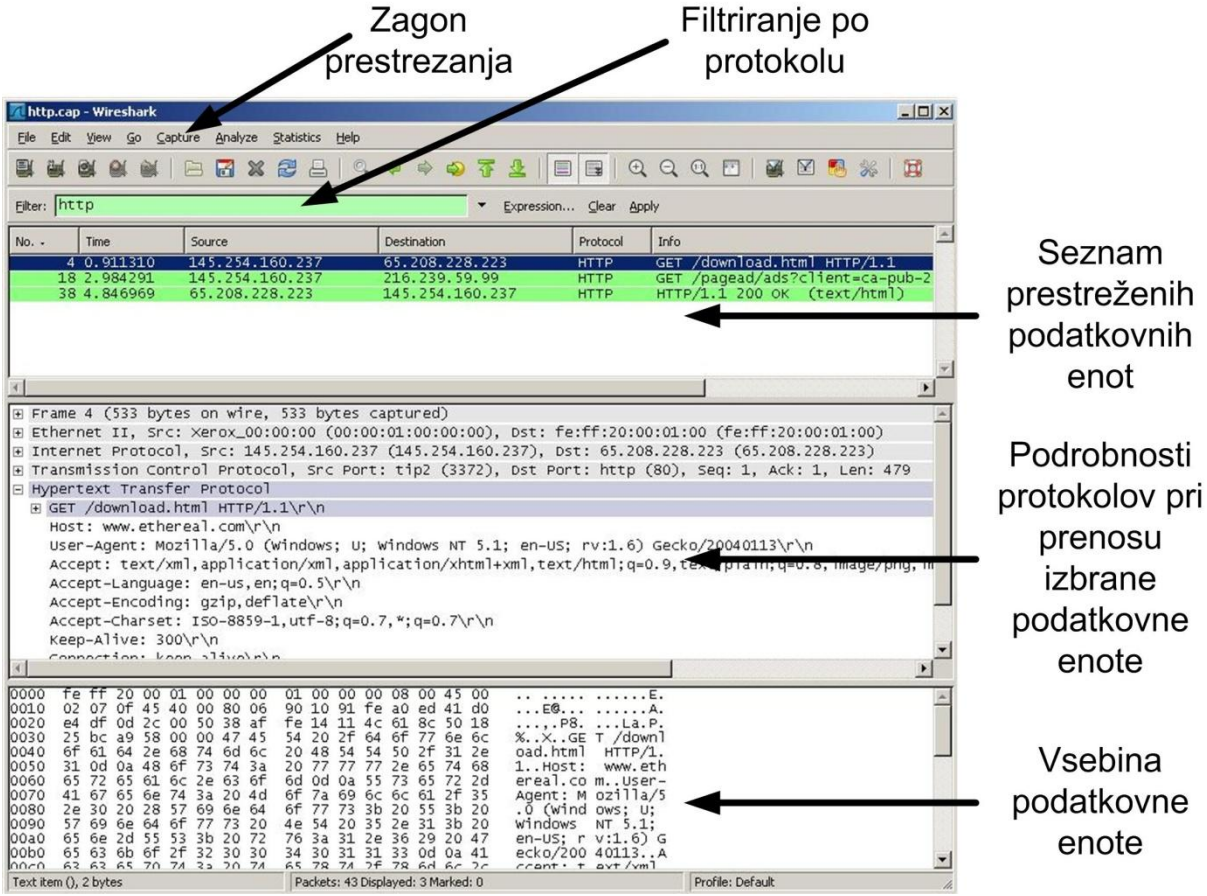
#### *Prestrezanje prometa*

a. Najprej določimo mrežni vmesnik na katerem bomo prestrezali promet: izvedemo ukaz **Capture|Interfaces** in izberemo želeni vmesnik (v našem primeru bo to mrežna kartica Ethernet).
b. Prestrezanje prometa začnemo z ukazom **Capture|Start** ali klikom na ustrezno ikono v orodjarni.
c. Prestrezanje zaključite s **Capture|Stop** ali klikom na ustrezno ikono v orodjarni.

*Uporaba preprostih filtrov*

Wireshark omogoča filtriranje prometa ob zajemu (capture) in ob prikazu (display). Slika 1 prikazuje uporabo prikaznega filtra, ki na zaslon prikaže samo podatkovne enote protokola HTTP. Bolj zahtevne filtre lahko naredimo tako, da kliknemo na gumb **Expression** in izberemo pogoje filtriranja.

Slika 1 prikazuje prestrežen promet in nekatere podrobnosti protokolov in podatkovnih enot.




**Slika 1: Analizator prometa in protokolov v omrežju (Wireshark).**

## *Naloge:*

1. Izdelajte filter, ki prikaže podatkovne enote protokola IP, ki imajo izvor ali cilj na vaši številki IP.
2. Izdelajte filter, ki prikaže komunikacijo z vašega računalnika na TCP port 80.

# 2 Prestrezanje nezavarovanih podatkov

Prenos nešifriranih podatkov preko nezavarovanih prenosnih poti je (lahko) nevarno početje. Poglejmo si dva primera prestrezanja nezavarovanih podatkov. Pri vseh primerih uporabimo program Wireshark.

## Prestrezanje gesla na nezavarovani povezavi

Poskusili bomo prestreči geslo uporabnika ob njegovi prijavi na strežnik FTP. Uporabili bomo program Wireshark in prestregli podatke prijave uporabnika na nezavarovani povezavi v lokalnem omrežju.

***Podatki o strežniku FTP:***

| | |
|---|---|
| naslov IP: | 212.235.190.214 |
| vrata: | 2121 |
| uporabnik: | vaje |
| geslo: | varkom |

## Naloge:

1. Nastavite prikazni filter tako, da bo prikazoval le podatkovne enote, ki se izmenjajo med našim računalnikom in strežnikom FTP.
2. Poženite prestrezanje prometa in se prijavite na strežnik FTP
3. Odjavite se s strežnika FTP in končajte s prestrezanjem prometa.
4. V prestreženih podatkovnih enotah poiščite uporabniško ime in geslo s katerim ste se prijavili na strežnik FTP.
5. Pridobite celotno komunikacijo med odjemalcem in strežnikom (Follow TCP Stream).

## Prestrezanje spletnih strani

Poskusili bomo prestreči ogledano spletno stran, ki deluje po protokolu HTTP. Ker prenos podatkov preko HTTP povezave ni zavarovan, ima vsakdo možnost prestreči promet med vašim računalnikom in spletnimi strežniki in tako dobi vpogled v vsebino komunikacije.

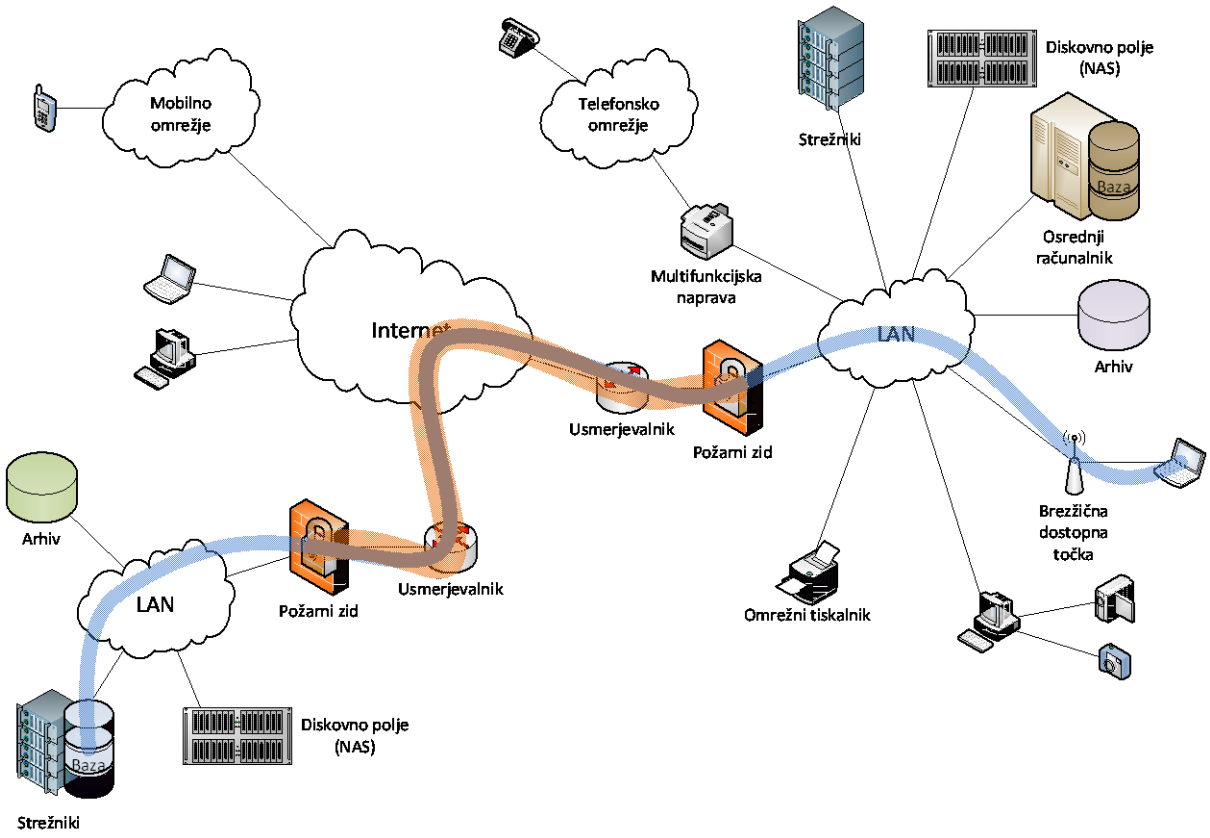
## Naloge:

1. Zaženite spletni brskalnik in počistite zasebne podatke (zgodovino, piškotke itd.).
2. Poženite prestrezanje prometa.
3. Filtrirajte podatke po protokolu HTTP.
4. Ugotovite kateri IP naslov ustreza vašemu računalniku in kateri je naslov strežnika, ki vam je posredoval spletno stran.
5. Viri, ki jih je spletni strežnik poslal vašemu brskalniku, so označeni kot HTTP/1.1 200 OK (vrsta dokumenta). Izmed vseh virov, ki jih je spletni strežnik posredoval vašemu računalniku, izberite prvega, ki se nanaša na HTML dokument (text/html) (Slika 2).
6. Z desnim miškinim gumbom kliknite na »line-based text data« v srednjem oknu in izberite **Copy|Bytes|Printable Text Only**.
7. Kopiran tekst shranite v nov HTML dokument in ga odprite z brskalnikom.

# 3 Vzpostavljanje varnih prenosnih poti

Vzpostavljanje varnih prenosnih poti pride v poštev predvsem pri prenosu podatkov preko omrežij, ki niso naša last. Največkrat je primer prenos preko omrežja Internet. Varnostna tveganja lahko odpravimo z vzpostavitvijo navideznega zasebnega omrežja (VPN), ki se večinoma izvedejo s pomočjo vzpostavljanja tunelov.

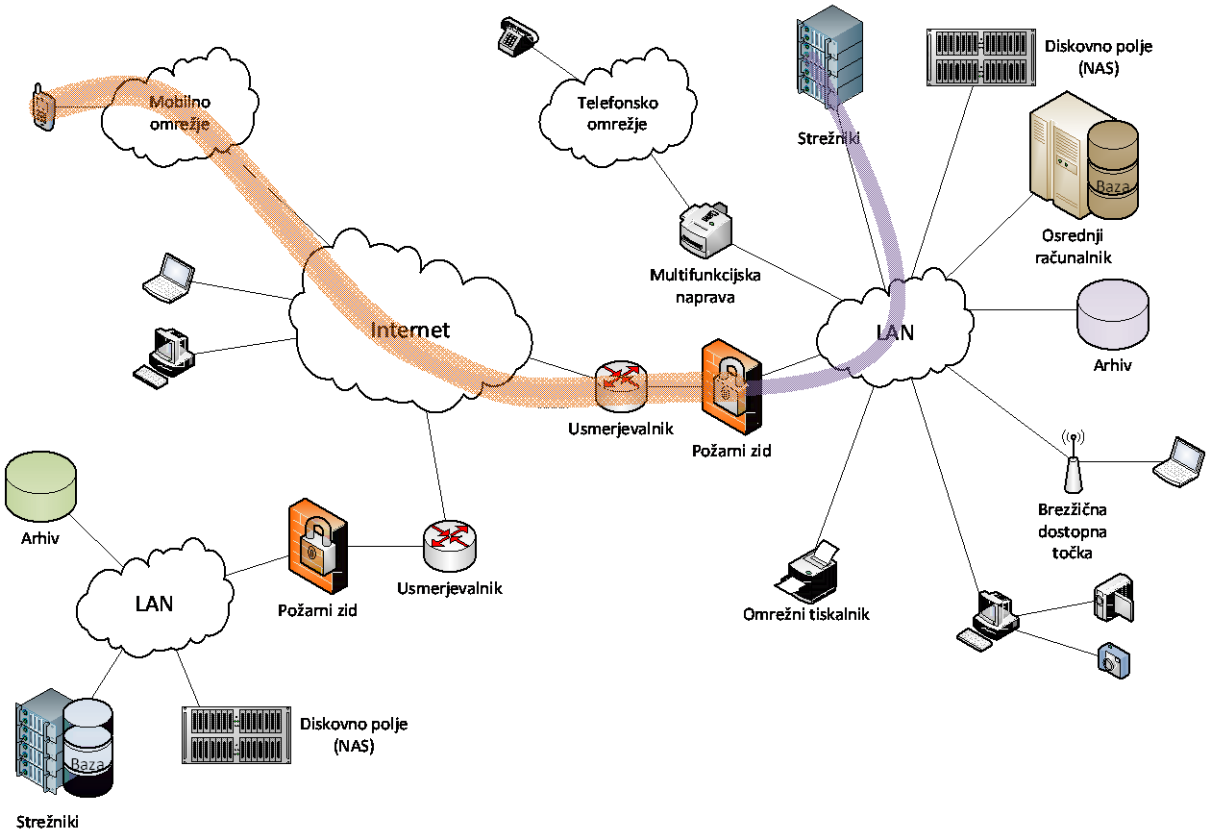
Slika 2 prikazuje primer, ko VPN vzpostavimo s pomočjo tunela med robnima usmerjevalnikoma ločenih delov zasebnega omrežja. Tipičen primer je povezovanje več oddaljenih lokacij nekega podjetja. Tunel je za promet transparenten in mora poskrbeti, da so podatki, ki se prenašajo skozenj, varni (šifrirani). Tunel je navadno vzpostavljen stalno.




Slika 2: Vzpostavitev tunela med robnima usmerjevalnikoma na ločenih delih zasebnega omrežja.

Slika 3 prikazuje primer, ko VPN vzpostavimo med končno napravo priključeno v (javno) oddaljeno omrežje in robnim usmerjevalnikom. Tipičen primer je povezovanje zaposlenih, ki se nahajajo na oddaljenih lokacijah, z zasebnim omrežjem podjetja. Tunel se navadno vzpostavi ob potrebi po izmenjavi podatkov in se po koncu le te poruši.

Obstaja cela množica načinov in protokolov za vzpostavljanje tunelov. Najpogosteje se uporablja protokol IPSec, ki izpolnjuje večino varnostnih zahtev, to je zaupnost, avtentičnost in verodostojnost podatkov, ki se prenašajo preko njega.




**Slika 3: Tunel med terminalom v (javnem) mobilnem omrežju in robnim usmerjevalnikom zasebnega omrežja.**

## *Vzpostavitev tunela in preverjanje njegove varnosti*

Vzpostavili bomo IPSec tunel med dvema računalnikoma na lokalnem omrežju in preverili prenos podatkov skozenj.

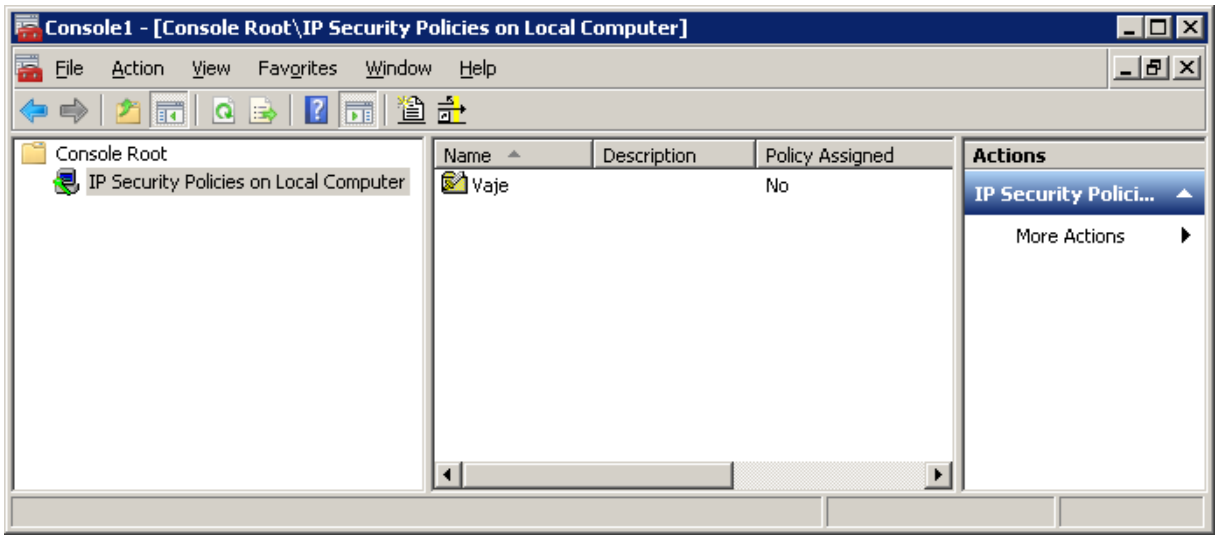
### *Vzpostavitev tunela IPSec med Windows 7 računalniki*

Z a vzpostavitev tunela med dvema Windows 7 računalniki je potrebno vzpostaviti ustrezne IP varnostne politike.

Odpremo Windows MMC (Microsoft Management Console): pojdite na **Start Menu**, v iskalno okence odtipkajte **MMC** in pritisnite Enter. Odpre se konzola. Izberite ukaz **File|Add/Remove Snap-in** in s seznama izberete **IP Security Policy Management** ter izberete **OK**.

Izberete ukaz **Action|Create IP Security Policy** in sledite čarovniku. Izberete **Next**, kot ime varnostne politike vpišete **Vaje**, dvakrat pritisnete **Next** in zaključite s **Finish** in **OK**.

Slika 4 prikazuje stanje konzole po izvedbi zgornjega postopka.



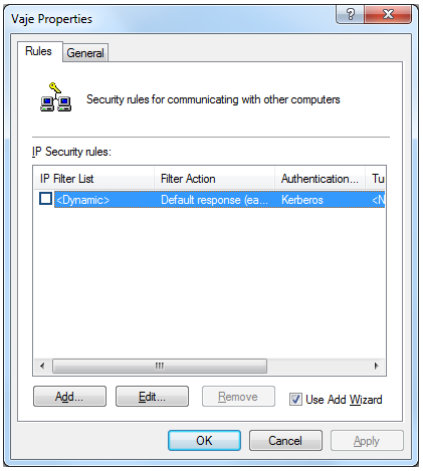

Slika 4: Vzpostavitev varnostne politike v Windows 7.

**Vzpostavitev tunela izvedite v parih – en par tvorita dva računalnika.**

Priporočeno je izbrati par, ki je čim bliže vašemu računalniku, idealno levi ali desni sosed, da v primeru nedelovanja lahko enostavneje preverjate nastavitve obeh računalnikov.

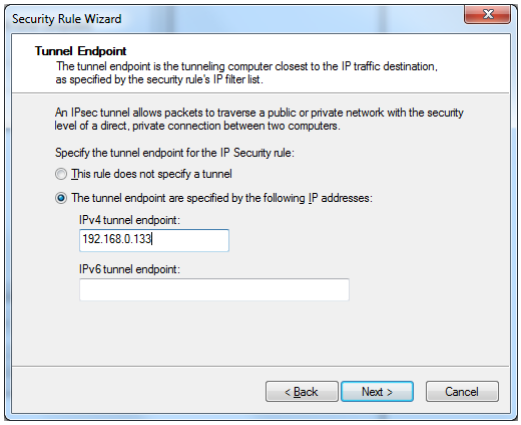
Znotraj ravnokar ustvarjene varnostne politike **Vaje** izdelamo tunel po naslednjih korakih, **ki jih izvedemo na obeh računalnikih v paru**:

Dvakrat kliknemo na ikono varnostne politike **Vaje**, izbrišemo vsa obstoječa varnostna pravila, razen tistega z oznako <**Dynamic**> (Slika 5).

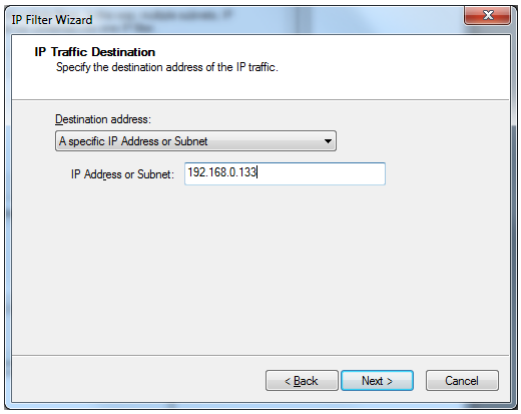



Slika 5: Elementi varnostne politike.

Nato z gumbom **Add** dodamo novo pravilo, ki bo veljalo v smeri od našega računalnika (**x**) proti računalniku, ki je z našim v paru (**y**). Zažene se čarovnik, izberemo **Next**, določimo, da bo pravilo določalo tunel in vpišemo konec tunela, ki je v našem primeru računalnik, ki je z našim v paru (Slika 6). Kliknemo **Next**, izberemo **All Network Connections**, izberemo **Next** in nato z gumbom **Add** dodamo nov filter za tunel. Določimo mu ime **IPxy** (smer od x proti y) in z gumbom **Add** določimo pravila. Najprej dvakrat kliknemo **Next** in nato kot izvorni naslov IP izberemo naš računalnik (x) – **My IP Address**, kliknemo **Next** in za ponorni naslov navedemo IP od računalnika v paru (Slika 7).



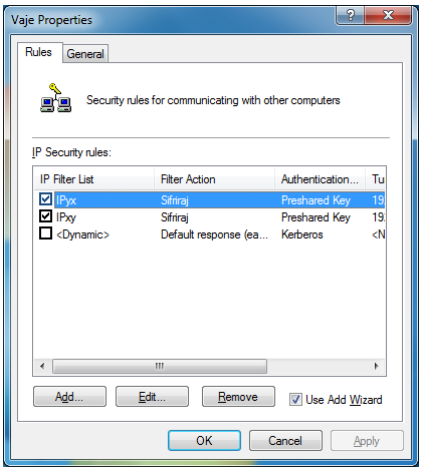

Slika 6: Določitev konca tunela.




Slika 7: Določitev konca tunela.

Kliknemo **Next**, določimo **Any** za tip protokola, kliknemo **Next**, **Finish** in **OK**. Izberemo pravkar izdelan filter **IPxy** in pritisnemo **Next**. Z gumbom **Add** dodamo novo akcijo, ki jo bo tunel izvajal nad prometom. Odpre se čarovnik, pritisnemo **Next** in določimo ime akcije **Sifriraj**. Pritisnemo Next, izberemo **Negotiate security**, potem **Next** in **Do not allow unsecured communication**, nato **Next** in **Integrity and encription**, **Next** in **Finish**. Izberemo akcijo **Sifriraj**, pritisnemo **Next** in izberemo **Use this string...** in v okence vpišemo ključ **test**. Pritisnemo **Next** in **Finish**. S tem smo zaključili izdelavo varnostnega pravila v smeri **x → y**.

Enak postopek izvedemo tudi za pravilo za smer y → x, pri čemer pa upoštevamo, da se izvor in ponor tunela zamenjata. Filter poimenujemo **IPyx**, za akcijo pa lahko uporabimo že izdelano akcoji **Sifriraj**. Na koncu postopka mora varnostna politika Vaje izgledati kot na sliki spodaj:




Slika 8: Elementi varnostne politike Vaje po končanih nastavitveh.

Kliknemo **OK**. S tem smo določili pravila varnostne politike **Vaje**, ki pa jo aktiviramo/deaktiviramo tako, da z desno tipko miške kliknema na njeno ikono in izberemo **Assign/Un-Assign**. Če je varnostna politika **Vaje** aktivirana na obeh računalnikih v paru, bo med njima potekala varna komunikacija skozi šifriran tunel. Če je vključena samo na enem, komunikacije ne bo potekala, Če bo na obeh izključena bo komunikacija nezaščitena.

### *Varen prenos podatkov skozi vzpostavljen tunel*

Preden se lotimo pošiljanja podatkov skozi tunel, moramo preveriti ali med računalniki na končnih točkah tunela lahko vzpostavimo komunikacijo. To bomo preverili s pošiljanjem ICMP sporočil **ping**. Ker pa imajo Windows 7 računalniki v osnovi vključen požarni zid, ki ne dovoljuje odgovorov na ICMP sporočila, moramo vzpostaviti novo izjemo, ki bo znotraj lokalnega omrežja to dovoljevala. Izvedemo ukaze:

- **Control Panel --> System and security --> Windows Firewall --> Advanced settings --> Inbound rules --> New rule --> Custom rule**,
- zatem v meniju **Protocol and ports** na levi izberemo **Protocol type: ICMPv4**,
- kliknemo **Next** in v naslednjem oknu
  - za local IP address izberemo Any IP address in
  - za remote IP address vpišemo naše lokalno podomrežje 192.168.0.0/24,
- nekajkrat kliknemo Next, določimo ime ICMP local in izjema je vzpostavljena.
- S sosedom preverimo ali se njegov računalnik odziva na naše ping-e.

## *Naloge:*

1. Vzpostavite IPSec tunel med vašim in sosedovim računalnikom.
2. Preverite povezljivost med obema računalnikoma:
   a. ko je tunel neaktiven,
   b. ko je tunel aktiven.
3. Z analizatorjem Wireshark spremljajte promet med računalnikoma in ga filtrirajte tako, da:
   a. boste spremljali samo promet protokola ICMP,
   b. boste spremljali samo promet med obema računalnikoma,
   c. boste zaznali promet skozi tunel.